What is your Exposure to Ransomware?

Assess your risk of ransomware attack.

What matters to your organization?

- Revenue
- Customer trust
- Business operations
- Compliance
- Reputation

What is your attack surface?

- Internet-facing systems
- Cloud services
- Third-party access
- Physical assets

How can you harden your attack surface?

- Network segmentation
- Access control
- Data encryption
- Patch management

How can you optimize your ransomware response?

- Incident response plan
- Business continuity plan
- Communication strategy
- Legal and regulatory requirements

What tools does your CISO have?

- Vulnerability management
- Threat monitoring
- Incident response
- Compliance monitoring

What is your attack vector?

- Phishing
- Malware
- RDP compromise
- Exploitation of software vulnerabilities

Do you continuously monitor for vulnerabilities?

- Patch management
- Software updates
- System configuration
- User behavior

What is your exposure to ransomware?

- 40% of ransomware attacks end in payment
- 60% of ransomware attacks end in data loss

How can you optimize your ransomware response?

- Early detection and response
- Information sharing
- Legal and regulatory compliance
- Business continuity planning

What regulations and compliance obligations do you have?

- PCI DSS
- GDPR
- HIPAA
- NIST

How do you assess the risk to your organization?

- Vulnerability prioritization
- Risk management
- Business impact analysis
- Compliance assessment

Can you map out the components of your critical services?

- Cloud services
- Network infrastructure
- Physical assets
- Third-party dependencies

Do you have any specialized skills or expertise?

- Cybersecurity
- IT operations
- Business continuity
- Legal compliance

How recently have you practiced your response?

- Annual
- Quarterly
- Monthly
- Weekly

Are you communicating during the process?

- Internal stakeholders
- External parties
- Stakeholder group
- defends on a single architecture with a common data model. With our ServiceNow workflows for security operations, IT, and risk management plan addressing the big picture of your cybersecurity.

ransomware readiness in key areas.

ServiceNow can help you orchestrate recovery efforts across your organization to respond to disruptions faster.

60% of breach victims said they were breached through a third-party vendor.

What is your attack vector?

- Phishing
- Malware
- RDP compromise
- Exploitation of software vulnerabilities

Do you continuously monitor for vulnerabilities?

- Patch management
- Software updates
- System configuration
- User behavior

What is your exposure to ransomware?

- 40% of ransomware attacks end in payment
- 60% of ransomware attacks end in data loss

How can you optimize your ransomware response?

- Early detection and response
- Information sharing
- Legal and regulatory compliance
- Business continuity planning

What regulations and compliance obligations do you have?

- PCI DSS
- GDPR
- HIPAA
- NIST

How do you assess the risk to your organization?

- Vulnerability prioritization
- Risk management
- Business impact analysis
- Compliance assessment

Can you map out the components of your critical services?

- Cloud services
- Network infrastructure
- Physical assets
- Third-party dependencies

Do you have any specialized skills or expertise?

- Cybersecurity
- IT operations
- Business continuity
- Legal compliance

How recently have you practiced your response?

- Annual
- Quarterly
- Monthly
- Weekly

Are you communicating during the process?

- Internal stakeholders
- External parties
- Stakeholder group
- defends on a single architecture with a common data model. With our ServiceNow workflows for security operations, IT, and risk management plan addressing the big picture of your cybersecurity.

ransomware readiness in key areas.

ServiceNow can help you orchestrate recovery efforts across your organization to respond to disruptions faster.

60% of breach victims said they were breached through a third-party vendor.

What is your attack vector?

- Phishing
- Malware
- RDP compromise
- Exploitation of software vulnerabilities

Do you continuously monitor for vulnerabilities?

- Patch management
- Software updates
- System configuration
- User behavior

What is your exposure to ransomware?

- 40% of ransomware attacks end in payment
- 60% of ransomware attacks end in data loss

How can you optimize your ransomware response?

- Early detection and response
- Information sharing
- Legal and regulatory compliance
- Business continuity planning

What regulations and compliance obligations do you have?

- PCI DSS
- GDPR
- HIPAA
- NIST

How do you assess the risk to your organization?

- Vulnerability prioritization
- Risk management
- Business impact analysis
- Compliance assessment

Can you map out the components of your critical services?

- Cloud services
- Network infrastructure
- Physical assets
- Third-party dependencies

Do you have any specialized skills or expertise?

- Cybersecurity
- IT operations
- Business continuity
- Legal compliance

How recently have you practiced your response?

- Annual
- Quarterly
- Monthly
- Weekly

Are you communicating during the process?

- Internal stakeholders
- External parties
- Stakeholder group
- defends on a single architecture with a common data model. With our ServiceNow workflows for security operations, IT, and risk management plan addressing the big picture of your cybersecurity.

ransomware readiness in key areas.

ServiceNow can help you orchestrate recovery efforts across your organization to respond to disruptions faster.

60% of breach victims said they were breached through a third-party vendor.

What is your attack vector?

- Phishing
- Malware
- RDP compromise
- Exploitation of software vulnerabilities

Do you continuously monitor for vulnerabilities?

- Patch management
- Software updates
- System configuration
- User behavior

What is your exposure to ransomware?

- 40% of ransomware attacks end in payment
- 60% of ransomware attacks end in data loss

How can you optimize your ransomware response?

- Early detection and response
- Information sharing
- Legal and regulatory compliance
- Business continuity planning

What regulations and compliance obligations do you have?

- PCI DSS
- GDPR
- HIPAA
- NIST

How do you assess the risk to your organization?

- Vulnerability prioritization
- Risk management
- Business impact analysis
- Compliance assessment

Can you map out the components of your critical services?

- Cloud services
- Network infrastructure
- Physical assets
- Third-party dependencies

Do you have any specialized skills or expertise?

- Cybersecurity
- IT operations
- Business continuity
- Legal compliance

How recently have you practiced your response?

- Annual
- Quarterly
- Monthly
- Weekly

Are you communicating during the process?

- Internal stakeholders
- External parties
- Stakeholder group
- defends on a single architecture with a common data model. With our ServiceNow workflows for security operations, IT, and risk management plan addressing the big picture of your cybersecurity.

ransomware readiness in key areas.

ServiceNow can help you orchestrate recovery efforts across your organization to respond to disruptions faster.

60% of breach victims said they were breached through a third-party vendor.